BEFORE THE FEDERAL COMMUNICATIONS COMMISION
WASHINGTON, DC 20554

In the matter of	:	CG Docket No. 17-59
Advanced Methods to Target and Eliminate Unlawful Robocalls	:	

COMMENTS OF VINCENT A. LUCAS

I thank the Commission for its work on addressing this issue. Americans are getting more unlawful, unwanted robocalls than ever.[1] Chairman Pai has expressed a strong interest in fixing this problem[2], and I find his statements highly encouraging. I propose several ideas in this paper. However, some of the ideas may be beyond the scope of what this Commission can do without action by Congress. Nevertheless, if this Commission were to make a report to Congress proposing the necessary legislative action, such report would have substantial influence in Congress.

I. Proposal 1: Make caller ID unspoofable. The problem of caller ID spoofing must be fixed, and can be fixed by using technologies already used in digital commerce

A. Spoofing is the key problem

The TCPA's statutory damages and penalties should be more than enough to eliminate robocalls. So why are people getting more robocalls than ever? The principal problem to both

[1] https://www.ftc.gov/es/about-ftc/bureaus-offices/bureau-consumer-protection accessed 7/2/2017.

[2] Remarks Of FCC Commissioner Ajit Pai At The First Meeting Of The Robocall Strike Force, 8/19/16 [https://apps.fcc.gov/edocs_public/attachmatch/DOC-340872A1.pdf]; Statement of Chairman Pai Re: Advanced Methods to Target and Eliminate Unlawful Robocalls [FCC-17-24A2.pdf]; Twitter feed of Chairman Pai [https://twitter.com/ajitpaifcc/status/766667688454283264]

blocking robocalls and enforcing the TCPA is that caller ID information can be spoofed. The current Caller Identification system is not designed to be reliable[3], and consequently illegal robocallers can avoid prosecution by caller ID spoofing and refusing to otherwise identify themselves during their calls. In addition, spoofers can readily evade efforts to block robocalls based on the telephone number of the call originator. For example, Nomorobo – winner of the 2012 FTC robocall challenge contest – attempts to block calls based on caller ID information. However, if caller ID information is unreliable, fraudsters will be able to find ways to get their calls through.

The problem with the FCC's proposed rule change is that, at best, it only puts a bandage on the real problem. The real solution is to change the caller identification system so that it is not spoofable. Fraudsters can still get around the proposed rules. For example, instead of using an invalid or unassigned telephone numbers as caller ID information, fraudsters can use a number that is assigned to someone else. For example, the Microsoft tech scammer could use an actual number for Microsoft tech support. Thus, if the proposed rule change is implemented, spoofers will adapt by changing their patterns for selecting what numbers to use, and hence the proposed rule change is likely to become obsolete before it is adopted.

B. Spoofing can be fixed

I have worked for over twenty years in computer science and hold a doctorate degree. I can therefore say authoritatively that there is no technological reason why caller ID cannot be made virtually unspoofable. The message spoofing problem has already been solved in digital

[3] Caller ID is easily spoofed using VoIP or PRI lines. See http://en.wikipedia.org/wiki/Caller_ID_spoofing. A Google search for "caller ID spoofing" shows many commercial websites claiming to offer Caller ID spoofing, e.g. http://www.spoofcard.com

commerce. The caller ID spoofing problem could be solved by applying the technologies used in digital commerce to the caller identification system. Think about it. Digital commerce simply could not work if it employed a system as unreliable as the current caller ID system. If digital commerce were as unreliable as caller ID, anyone could easily do a fraudulent money wire transfer by sending a message to a bank impersonating another bank.

In my submission to the 2012 FTC Robocall Challenge contest, I proposed a solution for fixing the caller ID spoofing problem.[4] In short, my proposal is that caller ID information be digitally signed by the telephone communications service provider of the call originator. A digital signature is a method used in digital commerce to authenticate that a message came from the person who the message purports to be from and that the message has not been altered by someone else.[5]

A Proposal for Authenticated Caller ID

When a telephone call is initiated:

1. The caller's communications service provider (CSP) sends a data message digitally signed by the caller's CSP. The data message contains, at a minimum:

    - the source (i.e. caller's) telephone number,

[4] https://www.ftc.gov/sites/default/files/documents/public_comments/2013/05/565017-00024-85937.pdf

[5] Digital signatures use private key/public key encryption. The sender has a private key that is secret. The sender uses the private key to encrypt a message. The message recipient uses a public key to decrypt the message. The public key can decrypt messages but cannot encrypt them. Thus, since the sender is the only one with the private key, the recipient can have confidence that the message truly did come from the sender. The recipient obtains the public key for the sender from a trusted third party, called a "Certificate Authority". For example, Verisign is one of the companies that acts as the Certificate Authority for Secure Socket Layer (SSL) communications. For telephone caller ID, the Number Portability Administration Center could act as the Certificate Authority. For more information on digital signatures, see e.g. H. Delfs and H. Knebl, "Introduction to Cryptography, Principles and Applications" (2nd ed. 2007); http://en.wikipedia.org/wiki/Digital_signature

- the name of the person or organization to whom the source telephone number has been assigned according to the records maintained by the caller's CSP (i.e. the name to display on the caller ID device),
- the destination telephone number, and
- a timestamp.

This data message is the Authenticated Caller ID information.

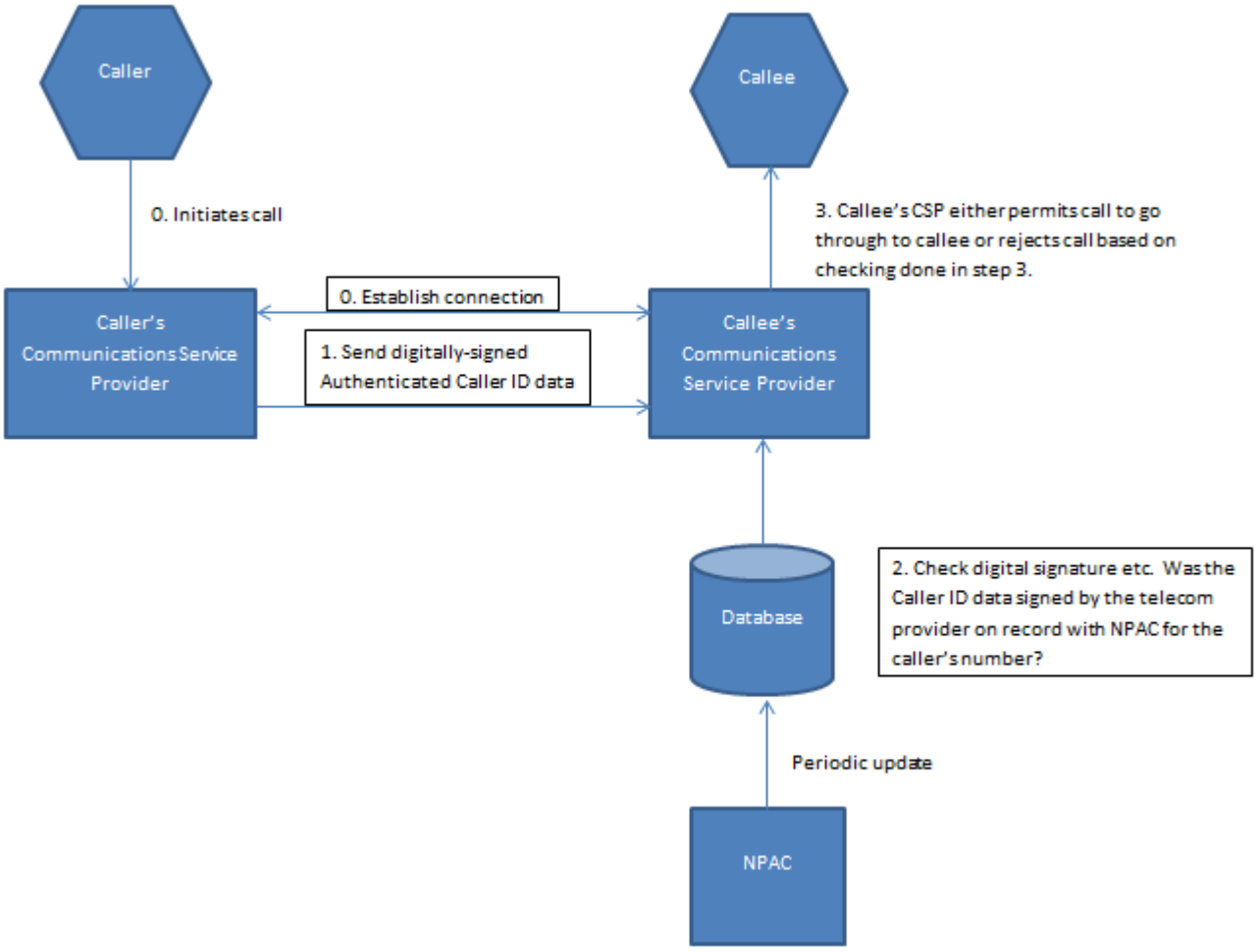
2. The destination's CSP rejects the data message if:

   - the digital signature is not valid;
   - the company that signed the data message is not the CSP associated with the source telephone number according to the records maintained by the Number Portability Administration Center (NPAC)[6]; or
   - the timestamp is more than 30 seconds[7] later than the time when the destination's CSP received the data message.

3. If the data message is not rejected, the destination's CSP permits the call to go through to the destination telephone. The source telephone number and name in the data message is displayed as the caller's phone number and name on the destination telephone's Caller ID device. If the data message is rejected, the call is terminated; the destination telephone does not ring and the callee is not otherwise alerted to the fact that someone attempted to call him/her.

[6] NPAC (http://www.npac.com) administers records that show what CSP a telephone number is assigned to. If a country other than the United States or Canada wants to provide Authenticated Caller ID information for calls originating from that country, the applicable regulatory agency in that country would need to use an organization similar to NPAC.

[7] The timestamp check is done so that the data message cannot be reused for a different call. A value other than 30 seconds could be used, but the value must be longer than the time required to transmit the message from the caller's CSP to the destination's CSP. On slow networks, one could also create a protocol to permit multiple attempts to retransmit the message if it is rejected only because of the timestamp



Responsibilities of the caller's CSP

The person or organization to whom the CSP assigned the telephone number is called herein the "account holder". The CSP shall maintain records that show the name and address of the account holder (and any other information designated by the FCC that would be useful to law enforcement in tracking down the account holder). The CSP should not be permitted to send a digitally-signed Authenticated Caller ID data message unless:

- For telephone numbers associated with a landline or cell phone, the call originates from the landline or cell phone associated with the account holder's telephone number;
- For telephone numbers associated with VoIP, the CSP has authenticated that the account holder, or someone authorized by the account holder, is the person originating the call, for example, the caller has logged into his account over a SSL connection using a reasonably strong password and then originates the call using the account.

This is not necessarily a comprehensive list. This Commission may find that there are other circumstances under which the CSP should be permitted to send the digitally-signed Authenticated Caller ID data message because under those circumstances there is high certainty that the call originates from the account holder, someone authorized by the account holder, or the account holder's telecommunication equipment.

These CSP responsibilities need to be enforced by FCC regulation, including liability and penalties for CSPs who willfully or recklessly violate the regulations.[8] A CSP that intentionally

[8] Some CSPs are VoIP service providers who have a strong financial incentive to assist telemarketers in evading telemarketing law. For example, some VoIP service providers receive revenue for each call because they are paid a fee by other CSPs for each Caller Name (CNAM) database lookup for one of their telephone numbers. Such providers have a strong financial incentive to seek clients who will make very high volumes of calls and encourage their clients to make as many calls as possible. For example, Stratics Networks and Star Networks are examples of CSPs that make money off of CNAM fees and encourage their clients to make high volumes of calls by sharing part of that revenue with their customers. See https://straticsnetworks.com/cnam-partner-revenue-sharing/ and http://starcompartners.com/cnam accessed 7/3/2017. Stratics Networks is one of the companies behind the All About The Message's FCC petition that was recently withdrawn due to an extraordinary outpouring of comments from the public opposing the petition. Another example is Net VoIP Communications. Net VoIP Communications is owned by someone who also operates a call center for Premium Outsourced Solutions, one of the perpetrators of the "Rachel" from Cardholder Services scam. See *Lucas v. Total Security Vision, Inc.,* No. 1:16-cv-1102, S.D. Ohio, Complaint.

For these reasons, it is imperative that this Commission impose liability on CSPs who are complicit in illegal telemarketing. The Commission made progress in this regard in Declaratory Ruling FCC 15-72 ¶ 30.

or repeatedly does not adhere to these responsibilities should be prohibited from being assigned telephone numbers by NPAC.

Business callers that wish to display a customized Caller ID number

Some business callers may wish to call from numerous telephone numbers but display on the Caller ID a single telephone number. E.g. calls from numbers 212-555-01xx all display as 212-555-0100 which is the customer service number for the business. This can be permitted, as long as the call originates from the business and the "display number" is assigned to the business according to the CSP's records. In this case, the Authenticated Caller ID message should contain both the number from which the call was actually sent ("From" number) and the number that the business intends to display on the Caller ID ("Reply to" number). This is analogous to e-mails that have a From field and a Reply To field. Legacy Caller ID display devices shall display the Reply To number. However, future Caller ID devices may display both the Reply To and the From number.

Handling calls that do not contain Authenticated Caller ID information

A call might not have Authenticated Caller ID information if the caller intentionally blocked the transmission of Caller ID information or the call originates from a region in which Authenticated Caller ID has not been implemented yet (e.g. a foreign country[9]). Telephone consumers should be provided, free of charge, an option to either automatically reject the call or permit it to go through. Other options could also be provided, such as permit the call if the

[9] I anticipate that if the United States adopts an Authenticated Caller ID system, most foreign countries will adopt the system. The U.S. frequently is the leader in telecommunications technology.

caller's number is on a list of numbers specified by the consumer. This option would be particularly useful to consumers who expect to receive calls from family and friends in regions where Authenticated Caller ID has not been implemented.

The consumer should be able to choose one of these options when setting up his/her telephone account, and should be able to change the option later.

User blocking of Caller ID information

Some consumers wish to occasionally block the transmission of the Caller ID information. This can be still permitted. However, the call will be rejected if the call recipient has set up automatic rejection of calls without Authenticated Caller ID information.

Extensions to consumer Caller ID display devices

Authenticated Caller ID should be implemented in a way such that existing caller ID display devices work. However, Authenticated Caller ID can transmit addition information that could be displayed on future caller ID devices, such as the "From number" when different than "Reply To number", the name of the CSP, the country of call origin, additional digits for international telephone numbers.

Feasibility of implementation

Authenticated Caller ID may require extensive changes, or a complete revamping, of the existing caller identification system. However, these changes are ultimately necessary in order to provide a true solution to the problem of targeting and eliminating robocalls. Authenticated Caller ID can be done in a way that is transparent to telephone customers. There will be

implementation cost to telephone service providers. But consider the cost to consumers of the current system. The IRS estimates that the IRS impersonation scam alone has cost victims $23 million.[10] Americans lose $8.6 billion per year to phone scams according to one estimate.[11] VoIP has allowed foreign telemarketers and con artists to make calls into the U.S. at little cost, and the current caller identification system allows them to make it appear that their calls originate in the U.S. and allows them to provide false caller name information to impersonate government agencies and legitimate businesses. This must come to an end. Authenticated Caller ID is the only way to bring it to an end.

This paper demonstrates that there is no technological reason why an Authenticated Caller ID system could not be implemented. What is needed is the willpower to make the necessary changes. The existing caller identification system needs to be replaced. Such sweeping change however is not unprecedented. For example, analog TV transmission has been replaced with digital transmission. Congress and this Commission saw that analog transmission was outdated and needed to be replaced, and did just that. Of course, there was some cost for the termination of analog transmission. Consumers had to either replace existing analog devices or obtain digital-to-analog converters. Television broadcasters had to make extensive changes. Certainly if this country can replace analog TV with digital, it can replace the current caller identification system with Authenticated Caller ID. The changes involved have to be far less extensive than the change from analog to digital TV. Unlike the digital TV conversion, consumers will not need to purchase new equipment to make use of the new caller ID system.

[10] https://www.irs.gov/uac/irs-urges-public-to-stay-alert-for-scam-phone-calls
[11] http://wjla.com/news/nation-world/phone-scams-cost-americans-8-6-billion-last-year-here-s-how-to-protect-yourself-106523

II. Proposal 2: Adopt my 2014 Petition for Declaratory Ruling regarding liability for persons who assist illegal telemarketing

In 2014, I submitted a petition asking for a declaratory ruling that "a person is vicariously or contributorily liable if that person provides substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates 47 U.S.C. § 227(b) or (c)." A ruling granting that petition with respect to persons who provide spoofing services[12] would substantially aid efforts to stop robocalls.

In 2015, this Commission's declaratory ruling FCC 15-72 ¶ 30 made several statements that providers of spoofing services may be liable.[13] The Commission was addressing "platform services", a term which is not defined in the ruling. However, one court has used FCC 15-72 in ruling against a Motion to Dismiss by an alleged provider of spoofing services.[14]

The Commission should confirm unambiguously that providers of spoofing services are liable under the TCPA. The 2015 Declaratory Ruling used the theory that such providers may be

[12] Spoofing services include, but are not limited to, services for transmitting false caller number or name information to caller ID devices and providing callers with "virtual telephone numbers" (such as numbers that are intended to be displayed on caller ID devices but which cannot receive incoming calls that connect to the party who used the virtual number for an outgoing call; and numbers that misrepresent the country from which the call originated)

[13] "Depending upon the facts of each situation, these and other factors, such as the extent to which a person willfully enables fraudulent spoofing of telephone numbers or assists telemarketers in blocking Caller ID, by offering either functionality to clients, can be relevant in determining liability for TCPA violations. Similarly, whether a person who offers a calling platform service for the use of others has knowingly allowed its client(s) to use that platform for unlawful purposes may also be a factor in determining whether the platform provider is so involved in placing the calls as to be deemed to have initiated them." Also footnote 110 says "For example, if the Commission staff notifies a platform provider that its service is being used unlawfully by its clients and the platform provider then allows such usage to continue after this warning, we will consider the fact that the platform provider allowed such usage to continue after having actual notice of the unlawful activity to be a possible indicator that the platform provider is actively participating in the making or initiating of the calls at issue."

[14] *Spiegel v. EngageTel*, No. 1:15-cv-01809 (N.D. Ill Sept. 29, 2016)(Doc. 134)

"so involved in placing the calls as to be deemed to have initiated them". My 2014 Petition provides an alternate argument for liability based on vicarious or contributory liability.

III. Proposal 3: There should be a legal presumption that spoofing is done for a fraudulent purpose

A major flaw of 47 U.S.C. § 227(e) is that it applies only when false caller ID information is transmitted "with the intent to defraud, cause harm, or wrongfully obtain anything of value." There should be a rebuttable presumption in the law that, when false caller ID information is transmitted, the intent is to defraud or cause harm. Similarly, when a person provides call spoofing services, there should be a rebuttable presumption that the person knows or should have known that the spoofing service is being used to defraud or cause harm. The presumption can be rebutted if the caller can prove that the false caller ID information is transmitted for a non-fraudulent, non-harmful purpose and was not used to attempt to wrongfully obtain anything of value.

IV. Proposal 4: When collecting upon a federal judgment for an intentional tort, state law exemptions to execution on assets should not apply

I recognize that this issue is beyond the authority of this Commission. However, this issue is part of the problem in enforcement of the TCPA, and a recommendation by this Commission for Congressional action on this issue would be very influential.

In my experience, a shocking number of telemarketers are located in Florida. The reason is that Florida has laws that can make it extremely difficult to collect upon a judgment. A person's homestead is exempt from execution, no matter what its value is. Telemarketers can

run their telemarketing enterprises out of million dollar mansions and consumers wrongfully injured by them can wind up with no monetary recourse. If the voters of Florida want their judgments against fellow Floridians who intentionally wrong them to be unenforceable, that is their problem. However, I didn't get a vote in the matter and I did not consent to receive calls from these Florida telemarketers. When a person in one state reaches into another state to commit an intentional tort under federal law, only federal exemptions to property execution should apply.

It is very strange that state law exemptions should even apply to executions on federal judgments. However, this is a consequence of the fact that the Federal Rules of Civil Procedure adopt the execution procedures of the states where the court is located. The Federal Rules of Civil Procedure should create federal procedures for judgment execution, and a practitioner should be permitted to choose to use either the federal or state law procedure. It is contrary to the supremacy of federal law that federal judgments against telemarketers can be effectively nullified by state law exemptions to execution. There is no Constitutional reason why this should be. The IRS is not encumbered by state law execution exemptions. So then, why should this Commission be encumbered by state law when it attempts to collect a statutory penalty? When private litigants win a TCPA judgment in federal court, why should they be encumbered by state law obstructions to judgment execution? After all, the TCPA is designed to enlist the aid of private litigants in enforcing the statute.

This proposal would also be helpful to businesses in general who are faced with collection against persons who deliberately shirk their legal responsibilities. In general, federal procedures for judgment execution would decrease the legal cost to companies of federal judgment execution.

Conclusion

These comments answer the Commission's call for "further steps the Commission could take to protect consumers and empower voice service providers to block illegal and fraudulent robocalls". NPR and NOI at 1. Parts of these proposals can be acted upon right away, such as making certain declaratory rulings. To the extent that the proposals require action from Congress, this Commission should issue a report to Congress strongly recommending the necessary legislative action.

Caller ID spoofing is the major impediment to TCPA enforcement and blocking unwanted calls. There is no technological reason why the caller identification system could not be made virtually unspoofable. This issue must be fixed.

Respectfully submitted,

Vincent A. Lucas, Ph.D.